360 终端安全防护系统
产品白皮书

适用版本：10.0.0.2200

版权声明

目 录

修订记录

版本	修订时间	编制者	审核者	修订内容
V2.3	*2021-9-30*			*更新 2200 版本内容*

1. 背景概述

目前国产操作系统在国家政策的推动下，已经逐渐的被国企事业单位使用，但其安全性因为没有验证过，反而比国外系统更令人生疑。比如易爆发各种安全问题，由于采用国产操作系统的用户不多，大多数软件未定期更新安全补丁，因此容易遭受攻击。而在专业计算机黑客的眼中，这些本土操作系统更容易出现安全漏洞，更容易收到恶意程序的威胁。

随着越来越多的服务器、移动设备、IoT 设备采用基于 Linux 内核的操作系统，针对 Linux 的恶意程序呈明显上升的趋势。从知名在线病毒检测网站 VirusTotal 的数据看，从 2017 年开始，Linux 恶意程序出现爆发式的增长。目前，已经发现的针对 Linux 的恶意程序主要有以下类型：

1、感染 ELF 格式文件的病毒

这类病毒以 ELF 格式的文件为主要感染目标，通过汇编或者 C 可以写出能感染 ELF 文件的病毒。

2、脚本病毒

脚本病毒是指使用 Linux shell 等脚本语言编写的病毒。此类病毒编写较为简单，不需要具有很高深的知识，很容易就实现对系统进行破坏，比如删除文件、破坏系统正常运行、甚至下载安装木马等。但它传播性不强，通常是在本机上造成破坏。

3、蠕虫病毒

Linux 系统下的蠕虫病毒与 Windows 下的蠕虫病毒类似，可以独立运行，并将自身传播到另外的计算机上去。蠕虫病毒通常利用一些操作系统和服务的漏洞来进行传播，比如，Ramen 病毒就是利用了某些版本的 rpc.statd 和 wu-ftp 这两个安全漏洞进行传播的。

4、后门程序

Linux 系统后门利用系统服务加载、共享库文件注射、rootkit 工具包、甚至可装载内核模块(LKM)等技术来实现，许多 Linux 系统平台下的后门技术与入侵技术相结合，非常隐蔽，难以清除。

5、勒索软件

近期一种新型的以加密受害主机文件向使用者勒索虚拟货币的恶意程序勒索软件开始盛行。勒索软件出现的初期仅仅针对 Windows 系统，但是从 2017 年的全球恶意软件统计分析中

可以得知，针对 Linux 系统的勒索软件开始规模性的涌现。相对其它传统的恶意程序，勒索软件通常会给用户带来直接的经济损失，需要重点防范。

总的来说，国产操作系统普遍采用 Linux 内核，有相当大一部分针对 Linux 系统的恶意程序都可以直接在国产操作系统上运行，并造成实际的危害。早在 4-5 年前，就有安全研究员发现有 Linux 样本利用技术手段很好地解决了跨平台的问题，也就是说同一个病毒样本，通过针对性的编译，可以运行在 X86、ARM、MIPS 等不同 CPU 架构的操作系统上。随着国产操作系统在党政军以及金融、能源等重要领域的大规模应用，可以预见专门针对国产操作系统的恶意软件也会呈现爆发式增长的趋势，我们需要为此做好准备。

当前，终端系统正在发生复杂深刻的变革，随着国产系统的大规模推广部署，国产系统也不可避免受到各类黑灰产组织的重视，如何有效解决国产系统的安全防护问题，是摆在安全管理员面前的重要课题。

为了解决国产终端的安全问题，360 集团充分发挥多年来积累的安全大数据、机器学习以及安全专家知识库的优势，发布了 360 终端安全防护系统软件与终端管理产品解决方案，旨在解决国产终端的安全防护难题。

2. 产品综述

2.1. 产品介绍

360 终端安全防护系统是 360 集团面向政府、军队、军工等企事业单位推出的以安全防御为核心、以安全策略管控为重点、以自动化运维管理为支撑的专业国产主机防护产品。可提供针对国产操作系统的病毒木马查杀、终端管控、安全审计等功能，能有效遏制内外部威胁的传播与扩散途径，全方位提升系统自身安全特性，确保内网终端和主机的安全。

2.1.1. 管理控制台

360 终端安全防护系统管理控制台部署在服务器上，正确部署后可实现对内部进行安全防护。管理控制台采用 B/S 架构，管理员可以通过浏览器打开管理界面，对安装 360 终端安全防护系统客户端的终端进行管理和控制。

2.1.2. 客户端

360 终端安全防护系统客户端软件部署在需要被保护的终端上，并与管理控制台通信，提供管理控制台管理所需的终端信息及日志。

2.2. 产品系统架构

360 终端安全防护系统主要由 360 终端安全防护系统统一安全管控中心、360 终端安全防护系统国产 Linux 杀毒终端及私有云服务器（选配组件）组成，产品架构图如下图所示：

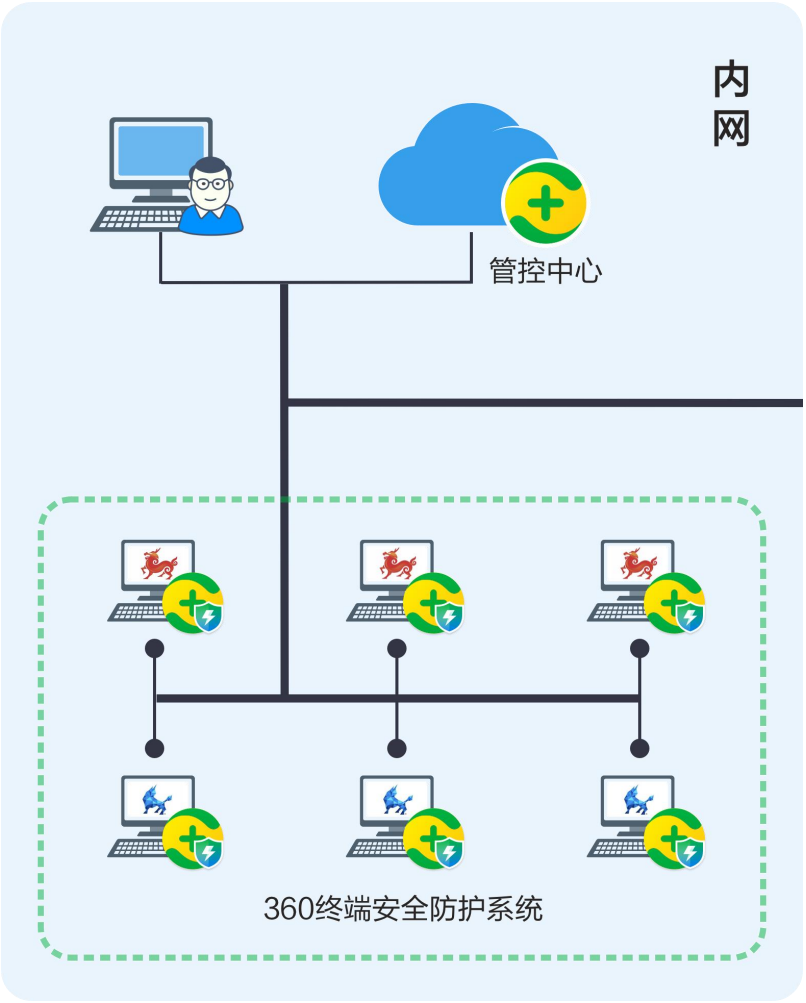

图 360 终端安全防护系统部署架构

2.3. 产品架构

图 360 终端安全防护系统产品功能框架

3. 产品功能

3.1. 平台管理

3.1.1终端概况

可以直观展示终端安全情况，包括终端信息和病毒信息。终端信息包括终端的操作系统分布比例、终端在线离线状态、客户端版本信息等。病毒信息包括病毒疫情情况、最新发现病毒、最新染毒终端、病毒类型统计、终端事件级别统计等信息。通过对全网终端安全情况的总览，方便管理员快速了解内网终端的安全状况，对发现的病毒及时进行处置。

3.1.2升级管理

可以查看终端病毒库的时间以及客户端版本，并对所选终端进行病毒库、客户端的升级。在隔离网场景，可以通过离线包的方式升级主程序版本及更新病毒库。

3.1.3任务管理

360 终端安全防护系统提供任务式管理功能，管理员可以创建计划任务，对指定组或终端下发病毒扫描、停止病毒扫描、消息推动、病毒库升级、客户端升级等任务，支持任务的启用、禁用、删除等操作。

3.1.4消息推送

消息推送能够方便管理员发送全局的消息通知，支持实时消息推送以及周期定时消息推送，实时消息推送可以实时对所选终端发布公告消息，能够定义有效期，有效期内终端皆可收到消息通知。周期定时消息推送可以针对分组或全网提前定义好通知，设置固定时间发送消息，如按周、按月固定一个时间点发送。

3.2. 防病毒

3.2.1 病毒扫描

360 终端防护系统内含多个领先的查杀引擎，包含云查杀引擎、鲲鹏引擎、QEX 脚本查杀引擎、QVM 查杀引擎，默认为引擎最佳组合，用户可根据自身电脑配置以及查杀需求进行相应调整。

病毒扫描：病毒扫描任务可以由管理员下发或终端用户主动扫描，时刻保障终端用户不受威胁。支持针对终端用户下发“快速扫描”、“全盘扫描”、“强力扫描”的扫描类型。

快速扫描：对终端下发指令，快速对终端系统目录，启动项，注册表，内存，易感染区等进行扫描，扫描范围固定，时间短。快速检查终端是否存在常见病毒；

全盘扫描：对终端下发指令，对终端全部路径进行文件扫描，确定终端是否存在病毒；

强力扫描：对终端下发指令，可以限制扫描模式为快速扫描或者全盘扫描，或自定义一个路径进行扫描，强力扫描能够忽略终端本地加白信任的文件或路径进行扫描。

灵活的病毒查杀与处理方式：在执行病毒查杀任务时，可以灵活选择病毒扫描资源占用速度最快或性能最佳的方式进行扫描。在发现病毒时，也可以灵活选择病毒处理方式，可选择由系统自动处理、由用户选择处理、仅上报但不处理等方式；扫描文件类型可选择仅程序和文档或所有文件进行扫描。

压缩包扫描：支持对压缩包扫描的设置，可以设置压缩包的扫描层数，压缩包的格式类型，最大扫描压缩包的大小。

隔离区恢复：可对终端被隔离的文件进行恢复。

信任区管理：支持添加文件夹以及文件全路径到信任区。

3.2.2 多引擎检测

360 终端安全防护系统包含技术先进的网络版防病毒功能，支持对蠕虫病毒、恶意软件、广告软件、勒索病毒查杀，这依赖于 QVM 人工智能引擎、云查引擎、鲲鹏引擎、QEX（针对非可执行文件的引擎）等多引擎的协同工作。

1、云查杀引擎

在隔离网环境，提供本地私有云，样本可以直接通过哈希比对进行黑白判定。如果终端能连接外部互联网，还能实现公云查杀，利用 360 云端海量样本资源进行恶意样本的检测。360 云查杀引擎建立在云端庞大的黑白名单数据库基础上，病毒检出率高，系统资源占用低。通过使用云端的黑白名单验证的方法，可以最大限度的保护数据安全。云查机制支持白亿黑白名单库，而且每天黑白名单库都在以百万级的数量在增长。

2、QVM 人工智能检测引擎

对于病毒和恶意代码的检测，一直存在着两个技术方向，一个是依靠病毒特征匹配的静态检测技术，这种技术的特点是必须依靠已知的病毒特征，一般静态特征匹配的技术适合对已知病毒、恶意代码的检测。另外一种是依靠对病毒行为的动态分析技术，这种技术更适合对未知病毒、恶意代码的检测。这两种技术是目前对病毒进行检测的关键技术，分别实现对已知、未知的病毒及恶意代码检测。

其中采用特征对病毒进行检测的技术又分为两个方向，一个是穷举式病毒特征提取，即针对每个已发现的病毒、恶意代码样本提取各自的病毒特征，这种方式的优点是能够准确识别出已提取特征的病毒与恶意代码，误报率和漏报率都很低。另一种是针对不同族类的病毒及恶意代码提取出共性的族群特征，并以此作为检测依据对恶意代码进行检测。这种方式的优点是不依赖某一个病毒或恶意代码的具体特征，而是提取某一族群的恶意代码共性特征，因此，这种检测方法对于某一病毒与恶意代码族群内的新生病毒具有非常强的检测能力，同时还能对检测出来的病毒与恶意代码进行族系归类。

QVM 人工智能检测引擎采用人工智能与机器学习的方法，对 360 目前已经积累的病毒样本进行多次切片学习，抽取出病毒与恶意代码的共性特征，建立恶意代码的不同族系模型，对变种病毒具有良好的检测能力。

3、鲲鹏引擎

鲲鹏引擎是依据以往 360 防病毒积累的技术和实力，面向政企隔离网使用环境开发的本地病毒查杀引擎。其在传统的本地查杀引擎技术的基础上，大量使用了大数据处理技术，是老技术和新技术的结合。

360 鲲鹏引擎，通过自主创新算法实现病毒库通杀型 1:1000， 引擎体积仅 80M 体量，为特征引擎中最小，病毒查杀速度最快的引擎。鲲鹏引擎具有以下特点：

1、依托 360 强大的数据收集和处理能力，利用大数据技术，实现精准地查杀。

2、相比于同类本地查杀引擎，在性能上具有显著优势。

4、EAV 引擎

EAV 引擎是依据 360 在防病毒方面的技术积累，自主研发的主要针对文件的专杀引擎，可以有效查杀 ELF 文件的病毒。

5、QEX 脚本引擎

针对非 PE 类宏病毒、VBS、REG 等恶意文件，360 终端安全防护系统利用专用 QEX 脚本查杀引擎进行检测。QEX 引擎既能结合精确特征和启发特征，来检出已知和未知的恶意威胁，又能对相关脚本模拟执行，根据输出结果做二次检查，确保结果的准确性。

3.2.3 实时防护

360 终端安全防护系统，提供对文件系统、压缩包等进行实时防护的功能。监控文件的类型，可选择全部文件或者仅监控程序和文档。在发现病毒时可以灵活选择病毒处理方式，支持选择由系统自动处理、由用户选择处理或仅上报不处理。支持对压缩包进行实时病毒防护，可配置监控压缩包的大小和层数。

3.3 终端管控

3.3.1 外设管控

对于隔离网用户来说，网内的安全风险往往是由移动介质引入的，对于 USB 移动设备的管理是防御外部风险的重要方式。

外设管控可以对 USB 存储设备进行管控，可以通过禁用终端 USB 接口的方式对接口进行控制，对内置光驱、U 盘等外设均能实现接口控制。

3.3.2 桌面安全加固

桌面安全加固能帮助企业的 IT 管理员对终端桌面系统的账号密码强度，密码有效期限等进行统一管控，并支持账号安全检测，降低恶意代码进行内部弱口令爆破的风险。协助 IT 管理员做到全网终端统一配置的管控目标，提高 IT 管理员的运维水平。

3.3.3 违规外联

伴随着互联网的发展，办公过程中对于互联网的依赖程度越来越高，同时，互联网也使

得恶意代码的传播与入侵越来越简易，360 终端安全防护系统为管理员提供了违规外联管控功能，通过对设备外联能力的探测，发现并处置正在进行违规外联的终端设备，一但发现终端尝试连接未经允许的网络地址，可以按需设置是否中断该设备的网络连接，避免恶意代码利用互联网及系统安全漏洞风险入侵内部办公环境，做到快速识别发现风险，并及时规避安全问题的产生，协助管理员解决网内恶意代码安全风险问题。同时管理员可以参照实际环境状况设置探测方式及时间间隔，保障安全检测的同时不会影响正常的日常办公需求。

3.4 移动存储管控

移动存储设备是内网重要的数据转移载体，对于移动存储设备，如果使用不当，容易导致外部病毒木马的入侵，同时容易造成内部重要数据的转移泄露。360 终端安全防护系统，提供包括 U 盘在内的移动存储设备的注册、识别和控制功能。管理员可以使用移动存储注册工具对 U 盘进行注册，在管理平台对注册的 U 盘进行使用权限的控制。

3.5 资产管理

资产管理记录终端的操作系统信息、硬件信息。平台具备跟踪硬件资产变更功能，可帮助管理员及时获取硬件资产的变更记录，硬件新增、丢失情况，对硬件变更准确监控。对操作系统版本、系统语言可进行记录，并可进行安装时间检测，相关信息可以导出供查看。

3.6 安全审计

安全审计能够对文档中的关键字进行审计，对终端下发安全审计的任务，对终端上文档中的关键字进行扫描，支持对 word，WPS 和 ODF 的文件的关键字审计。并且支持自定义需要审计的词库。

4. 产品价值

4.1. 全面的风险监测能力

360 终端安全防护系统采用动静结合的多层次、全生命周期的病毒防御体系。结合了传统

本地查杀引擎、360 公有云查杀引擎、QVM 机器学习查杀引擎,对病毒及恶意代码从终端落地、运行时的不同阶段进行多层过滤、动静结合、全程查杀，有效提升国产终端的病毒防御能力。

4.2. 强大的兼容适配能力

360 终端安全防护系统具备强大的环境兼容适配能力，针对国产化平台、操作系统及数据库应用等已进行了全面兼容适配工作，兼容支持龙芯、飞腾、兆芯、鲲鹏、海光等国产化芯片，同时适配了中标麒麟、银河麒麟、统信 UOS 等国产化操作系统，数据库方面，可以支持达梦数据库、人大金仓数据库、神州通用数据库等国产化数据库，并且还在不断适配更多的国产化环境，有效解决系统中心环境内复杂多变的软硬件系统环境安全防护问题。

4.3. 终端合规管控能力

360 终端安全防护系统具有丰富的管理功能，友好的用户界面，通过移动存储管控、违规外联管理和桌面加固的能力，对终端进行合规管理，规避政策风险，促进安全合规。